The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

DATE(S) ISSUED:
4/9/2010
4/15/2010 - ***UPDATED***

SUBJECT:
Multiple Vulnerabilities in the JRE Java Platform Could Allow Remote Code Execution

ORIGINAL OVERVIEW:
Multiple vulnerabilities have been discovered in the Oracle Java (formerly known as Sun Java) Runtime Environment (JRE) that could allow attackers to take complete control of a vulnerable system. The Java Runtime Environment is used to enhance the user experience when visiting web sites and is installed on most desktops and servers. These vulnerabilities may be exploited if a user visits or is redirected to a specifically crafted web page, or opens a specially crafted file. Successful exploitation could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Failed exploit attempts may result in a denial-of-service condition.

Proof of concept code for this vulnerability has been published and is publicly available. This code has been verified in our lab in a Windows environment and confirmed to cause remote code execution. Due to the ease in which this vulnerability can be exploited, we believe it is likely that this attack will be seen in the wild.

UPDATED OVERVIEW:
Oracle has indicated that Java Runtime Environment 1.6.0_20 (JRE 6 Update 20) has resolved this vulnerability. We have tested the JRE 6 Update 20 in our lab environment to confirm that it does resolve this issue.

Please note that we have received reports of this vulnerability being used to actively compromise systems on the Internet.

ORIGINAL SYSTEMS AFFECTED:

JRE 1.6 Update 10 and Later

UPDATED SYSTEMS AFFECTED:
JRE 1.6 Update 10 – JRE 1.6 Update 19

RISK:

Government:
Large and medium government entities: **High**
Small government entities: **High**

Businesses:
Large and medium business entities: **High**
Small business entities: **High**

Home users: High

ORIGINAL DESCRIPTION:
Multiple vulnerabilities have been discovered in the Java Runtime Environment (JRE) applications that could allow attackers to execute remote code on a system. The JRE allows a user to run Java applications, including web programs called applets, which are used on many websites.

These remote code execution vulnerabilities are due to insufficient validation of user-supplied input passed to the 'launch' function of the Java Deployment Toolkit plugins and the 'docbase' and 'launchjnlp' parameters of the Java Platform SE plugins. After the input is passed to the plugins, an attacker can exploit these issues to pass arbitrary arguments to the 'javaws.exe' command. This vulnerability can be further leveraged to execute arbitrary JAR or DLL files through the use of the '-J', '-XXaltjvm' and '-J-XXaltjvm' parameters. These vulnerabilities may be exploited if a user visits or is redirected to a specifically crafted web page, or opens a specially crafted file. Successful exploitation could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Failed exploit attempts may result in a denial-of-service condition.

The following plugins are affected and installed by default in the JRE:

deploytk.dll
This is a Java Development Toolkit plugin for Internet Explorer implemented as an ActiveX control identified by CLSID: {CAFEEFAC-DEC7-0000-0000-ABCDEFFEDCBA}

npdeploytk.dll
This is a Java Deployment Toolkit plugin for Mozilla Firefox implemented as an Netscape Plugin Application Programming Interface (NPAPI) plugin.

npjp2.dll
This is a Java Platform SE plugin for Mozilla Firefox and Google Chrome.

jp2iexp.dll
This is a Java Platform SE plugin for Internet Explorer implemented as an ActiveX control identified by CLSID: {8AD9C840-044E-11D1-B3E9-00805F499D93}

Proof of concept code for this vulnerability has been published and is publicly available. This code has been verified in our lab in a Windows environment and confirmed to cause remote code execution. Due to the trivial nature of this exploit, we believe it is likely that this attack will be seen in the wild.

UPDATED DESCRIPTION:
Oracle has indicated that Java Runtime Environment 1.6.0_20 (JRE 6 Update 20) has resolved this vulnerability. We have tested the JRE 6 Update 20 in our lab environment to confirm that it does resolve this issue.

Please note that we have received reports of this vulnerability being used to actively compromise systems on the Internet.

ORIGINAL RECOMMENDATIONS:
We recommend the following actions be taken:

- Set the kill bit on the Class Identifier (CLSID) {CAFEEFAC-DEC7-0000-0000-ABCDEFFEDCBA}; further instructions on how to set the kill bit can be found at the following location (http://support.microsoft.com/kb/240797).

- Mozilla Firefox and other NPAPI based browser users can be protected using File System ACLs to prevent access to npdeploytk.dll. These ACLs can also be managed via Group Policy Objects.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to download or open files from un-trusted websites.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Apply appropriate patches provided by Oracle to vulnerable systems as soon as they become available.

UPDATED RECOMMENDATIONS:
The following actions should be taken:

Systems running JRE 1.6 Update 10 - JRE 1.6 Update 19 should be updated to JRE 1.6 Update 20.

ORIGINAL REFERENCES:
Security Focus:
http://www.securityfocus.com/bid/39346

Full Disclosure:
http://seclists.org/fulldisclosure/2010/Apr/119

Ruben Santamarta:
http://www.reversemode.com/index.php?option=com_content&task=view&id=67&Itemid=1

UPDATED REFERENCES:
Oracle:
http://blogs.oracle.com/security/2010/04/security_alert_for_cve-2010-08.html

Security Focus:
http://www.securityfocus.com/bid/39346

US-CERT:
http://www.kb.cert.org/vuls/id/886582